



The Urgency of the Indonesian Non-Penal Policy in Regulating Misuse of Bank Accounts as a Means of Online Frauds

Rahel Octora

Faculty of Law-Universitas Kristen Maranatha

Email: octora@gmail.com

ORCID: <https://orcid.org/0000-0002-6966-2358>

Demson Tiopan

Faculty of Law-Universitas Kristen Maranatha

Email: demson.tiopan@yahoo.co.id

ORCID: <https://orcid.org/0000-0003-2446-8591>

Shelly Kurniawan

Faculty of Law-Universitas Kristen Maranatha

Email: shellyelvira@gmail.com

ORCID: <https://orcid.org/0000-0003-3239-5329>

Hassanain Haykal

Faculty of Law-Universitas Kristen Maranatha

Email: hassanain.haykal@gmail.com

ORCID: <https://orcid.org/0000-0002-4344-4598>

P. Lindawaty S. Sewu

Faculty of Law-Universitas Kristen Maranatha

Email: lindawatysewu@gmail.com

ORCID: <https://orcid.org/0000-0003-0258-7450>

Christian Andersen

Faculty of Law-Universitas Kristen Maranatha

Email: andersen.xtian@gmail.com

ORCID: <https://orcid.org/0000-0002-5974-5803>

Yohanes Hermanto Sirait

Faculty of Law-Universitas Kristen Maranatha

Email: yohanessirait1988@gmail.com

ORCID: <https://orcid.org/0000-0001-5678-3188>

Abstract

Key words:
Indonesia, non-penal, policy, misuse, bank account, fraud.

As the number of online transactions increases, so is the possibility of fraud. There are no face-to-face encounters, and the money is made through bank transfer. Fraudsters utilize a bank account to store their illicit funds. Currently, Indonesia's many laws and regulations cannot combat the numerous online frauds. When fraud occurs, it is usually difficult for the money sender (the victim) to get their money back. On the other hand, it is straightforward for a fraudster to obtain the funds deposited into their account and enjoy the fruits of their crime. This research was conducted utilizing a normative juridical methodology, and the consistency of policies in various Indonesian laws and regulations was investigated. This article contains doctrinal law studies about legal ideas, concepts, and rules. This study utilized legal documents such as statutes, journals, and other relevant publications. This study aims to examine the numerous Indonesian legal rules and their application in relation to the topic at hand. The outcomes of this research are recommendations for policy formulation, encompassing both penal and non-penal policies. The government must develop banking sector policies, account opening policies, and a system for blacklisting account owners whose accounts have been exploited for fraudulent purposes. The government must also establish more accessible and straightforward methods for reporting crimes.

Introduction

A bank is crucial to the economic growth of a nation. Bank provides a variety of payment options. Banks facilitate money transfer operations in the middle of a trend of online transactions. After an agreement has been reached, the following stage is the payment procedure, which can be conducted via a money transfer mechanism (Demirgüç-Kunt, Pedraza, & Ruiz-Ortega, 2021; Hidajat & Lutfiyah, 2022; Setyaningsih & Marwansyah, 2019). One customer's account can be transferred to another customer's account at the same or a different bank. In Indonesia, the movement of funds is governed by Act No. 3 of 2011 about Funds Transfer.

There are several instances of online sales and purchases fraud in Indonesia. The Directorate of Cyber Crimes, Criminal Investigation Division, recorded 1,617 online frauds in 2019. Instagram had 534 (five hundred and thirty-four) cases, WhatsApp had 413 (four hundred and thirteen), and Facebook had 304 (three hundred and four) cases (Ramadhani, 2020). According to data from the Ministry of Commerce, as of the first semester of 2021, 4,855 (four thousand eight hundred and fifty-five) consumers had filed online fraud complaints. The Ministry of Communication and Information Technology received 115,756 allegations of online transaction fraud in 2021. (Contributors., 2021)

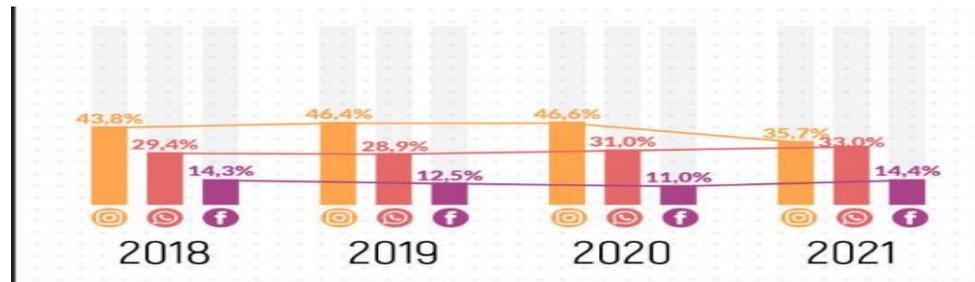


Figure 1. Platform used as means of online fraud (source: tirtoco.id)

In Indonesia, numerous fraudsters exploit the funds' transfer function to get money through fraudulent online sales and purchases fraudulently. The victim transfers funds as payment for things that do not exist. Fraudsters utilize various methods to ensure that the fraudulently obtained funds are soon under their control and that the victims cannot retrieve the funds that have been transferred to the fraudster's account. A fraudster frequently uses a bank account from a different institution than the victims. The fraudster withdraws the money immediately after receiving it, while the victim has no legal protection. The Indonesian Funds Transfer Act controls the methods of money transfer, beginning with the sender, sender's bank, receiver's bank, and ending with the fund recipient. However, it does not address the potential of a fraudulent transfer order cancellation. This makes it challenging for the victim of fraud to obtain legal protection.

Many online frauds are outside the grasp of legal enforcement (Lee, 2009). People still have minimal understanding and concern for reporting cybercrime to law enforcement. Some believe it is useless to report the incidents because the amount of money they lose is minimal. Additionally, they believe that if the case is brought to court, they will lose more than they win. People should report cybercrimes to the police to assist law enforcement in eradicating cybercriminals roaming the internet. (Rahmanto, Kav, & Kuningan, 2019)

Given the preceding explanation, it is evident that Indonesia must establish a policy to eradicate crime. The criminal policy is a nation's reasonable effort to combat crime. (Ravena, 2017). According to Barda Nawawi Arief, there must be an integration between the attempt to eradicate crime and the use of penal and non-criminal law or non-penal policy. (Arief, 1992)

Indonesia is a country that follows the Civil Law legal tradition. The written law, including criminal law regulations, is relatively comprehensive. The criminal consequence for online fraud is governed by Act No. 11 of 2008, as revised by Act No. 19 of 2016 respecting Electronic Information and Transaction, regarding the use of punitive measures. The current rule is a criminal regulation applicable to fraud. In light of the employment of non-punitive measures, the rule that can aid in eradicating online fraud is still considered suboptimal. One relates to the rule regarding the revocation of fraudulent fund transfer orders.

In addition, the law enforcement process for internet fraud in Indonesia will continue to follow the traditional method, which begins with a police report. This is one of the obstacles to Indonesian law enforcement. Those who commit crimes through technology should face a law enforcement system also assisted by advanced technology. Currently, when a perpetrator and victim are in different areas, the victim must report the crime to the police station in the victim's residence. The criminal proceedings will be conducted following the Criminal Procedure Code.

Due to the limited information on which the victim's report is based, the law enforcement process will encounter numerous challenges, one of which is the inability to determine the whereabouts of the culprits. The only information the victim has is related to the social media utilized to perpetrate the fraud and the bank account of the recipient of the funds. The social media account can be deactivated or erased to remove any traces. In addition, it is possible that the bank account is not the account of the fund recipient but someone else's.

According to the applicable regulation, which is Article 12 paragraph (1) of Bank Indonesia Regulation Number 2/19/PBI/2000 concerning Regulation of Bank Indonesia Number 2/19/PBI/2000 concerning Requirements and Procedures to Grant Written Orders or Approval to Disclose Bank Secrets, the blocking or confiscation of the deposit of a customer who has been declared a defendant or suspect by the police, prosecutor, or judge may be carried out following the rules of the applicable jurisdiction. However, this does not fix the issue if the criminal withdraws the proceeds of the crime in cash and then allows the blocking to occur. As a significant legal development, Bank Indonesia and the Bye-Laws Committee issued a decree in December 2009 declaring that customers who become victims of fraud can request the bank to block or temporarily terminate the criminal's bank account. The victim must still report the transaction to the authorities, and the bank will verify the transaction on the criminal's account.

This paper addresses how legal rules in Indonesia might safeguard fraud victims and how law enforcement could crack down on frauds using internet transactions and exploiting bank accounts to conceal illicit funds. This research is essential due to the escalating number of occurrences of online fraud in Indonesia and the lack of a legal remedy capable of protecting victims. The government is anticipated to apply the policy recommendations from this research to harmonize numerous laws and regulations. This work is organized as follows: introduction, literature review, methodology, analysis, and discussion followed by conclusions and recommendations.

Literature Review

We will first briefly discuss several earlier research pertinent to this topic before moving on to the description connected to the literature study.

1. Initiatives to Prevent E-Commerce Fraud Based on Indonesian Cyber Law, published in 2021 at the 9th International Conference on Cyber and IT Service Management, by Yanto Sufriadi, Faculty of Law, Universitas Prof. Dr. Hazairin SH, Bengkulu, Indonesia (CITSM). Based on Indonesian Cyber Law, this study focuses on the issue of preventive measures in law enforcement against e-commerce fraud. [Sufriadi \(2021\)](#)

2. Asif Lutfiyana from the Indonesian Data Privacy Research Center, "Online Buying and Selling Fraud in Indonesia and Its Criminal Law Enforcement," published in Law Research Review Quarterly, 7(1), 2021. The study stressed and discovered that there is always a potential for criminality to manifest itself in any service provided by an internet firm. As a result, the government created Law Number 11 of 2008 Concerning Electronic Information and Transactions as a regulation. Nevertheless, this regulation has to be revisited, as there are still gaps in its ability to prosecute cybercrime. [Lutfiyana \(2021\)](#)

Our research focuses not only on cyber law but also on fund transfer legislation and banking law, which is different from previous research in that we concentrated on examining the synchronization of policies contained in multiple laws and regulations. Following Act No. 7 of 1992 Concerning Banking regulations, a bank is an intermediary institution. According to Article 3 of Act Number 7 of 1992, the primary role of banking in Indonesia is to gather and distribute public monies. A bank is referred to as an intermediary institution if it acts as a collection point for savings from customers (savings accounts, current accounts, and time deposits) and disburses the funds to customers through credits. 2019's Hadi Ismanto Moving money is another aspect of a bank's activity, both for its benefit and that of the public ([khan, 2022](#); [Shafique & Khan, 2020](#); [Shaikh, 2018](#); [Younas & Kalimuthu, 2021](#)). The transfer is a method that can be used to move money.

Society has changed as time goes by. Technological innovation greatly supports people's activities ([Lee, 2009](#)). At this time, Indonesia has entered the digital economy age, where the influence of information technology permeates all aspects of economic activity. 268,583,016 people make up the nation of Indonesia. Internet usage is widespread in Indonesia. According to data from the Indonesian Internet Service Provider Association (or APJII), 196,714,070 (one hundred and ninety-six million, seven hundred and fourteen thousand, and seventy) people, or roughly 73.2% (seventy-three-point two percent), of Indonesians used the internet in the second quarter of 2019-2020. Indonesia Survey Center and the Indonesian Internet Service Provider Association, 2020).

This unquestionably affects how a financial transaction is carried out. Business transactions involving money transfers are common. A transaction's payment is often made utilizing the funds' transfer method from the bank account of the party responsible for making the payment to the account of the party entitled to receive it.

Without face-to-face interaction, the parties involved will conduct transactions that undoubtedly carry some risk. Numerous frauds are occurring in the transaction procedure right now. As the pattern of online transactions between business operators and customers develops, so does crime. Frauds are crimes that are frequently discovered. According to Indonesian criminal law, fraud is prohibited under Article 378 of the Criminal Code, which reads as follows:

"Any person who with intent to unlawfully benefit himself or another, either by assuming a false name or a false capacity, or by crafty artifices, or by a web of fictions, induces someone to deliver any property or to negotiate a loan or to annul a debt, shall, being guilty of fraud, be punished by a maximum imprisonment of four years."

It is crucial to demonstrate that the offense described in Indonesia's Criminal Code, Article 378, involved cunning artifices or a web of lies that led the victim to donate something to the offender (criminal). Article 28 of Law No. 11 of 2008 Concerning Electronic Information and Transactions (from now on IET Law), as most recently amended by Act No. 19 of 2016 Concerning Law No. 19 of 2016 Amendments to Law No. 11 of 2008 Concerning Information and Electronic Transactions (from now on IET Law), which regulates illegal acts, includes a provision that states: "Any person intentionally, and without right, spreading false and misleading information which causes confusion, misinformation, or panic, or which is likely to mislead.

The current method of sale and purchase is for the vendor to advertise the goods on social media and the customer to contact the seller using a communication app (Demirgüç-Kunt et al., 2021; Hidajat & Lutfiyah, 2022; Setyaningsih & Marwansyah, 2019). If they are successful, the deal is finalized, and the transfer method is used to collect payment. Because buyers must send funds first, while the items are still under the seller's control or possibly never exist, this puts them in danger. Currently, several marketplaces include "marketplace bank accounts" to keep funds so that, if the buyer has already received the good, the seller will receive the funds. According to the explanation mentioned above, there are 2 (two) reasons why people commit online scams. They are:

1. Internal factors, such as not genuinely trying to scam, the victim's carelessness, and the limited proportion of internet fraudsters arrested by the authorities.

1. Outside variables, such as the economic and environmental context of online fraudsters.

Methodology

Normative and sociological legal research set the current legal research

models apart. Differentiation from the perspective of the law's own research goals. Research on the synchronization of law, systematic study of law, the study of legal principles, the study of legal history, and comparative law are all examples of normative legal research. While sociological or empirical research focuses on the effectiveness of the law and the examination of legal identity (which is not written). [Christiani \(2016\)](#). Finding legal rules, doctrines, and principles to solve the current legal difficulties is the process of normative legal research. The argument, hypothesis, or novel idea that emerges from the study of law serves as a prescription for resolving issues [Marzuki \(2005\)](#). This study is normative. It is also classified as library research. Statutory and conceptual techniques are employed. These methods enable the analysis of normative rules based on the applicable laws and regulations. A conceptual approach necessitates the study team's use of legal precedents. The purpose of this research is to identify legal rules and policies that can be used to address legal issues. Hence it looks at legal standards, legal principles, and regulations. This study is not intended to determine if the law is effective. Hence it cannot be categorized as empirical research.

Results and Discussion

To understand how the Indonesian legal policies, both the penal and non-penal policies, overcome the misuse of bank accounts as a means to keep the funds resulting from online fraud, this paper will analyze:

1. Regulation of Sale and Purchase Activities and Funds Transfer in Indonesia
2. Regulation of Opening a Bank Account
3. Procedures of Law Enforcement in Cases of Misuse of Bank Accounts

Analysis of Regulation of Sale and Purchase Activities and Funds Transfer in Indonesia

Act Number 3 of 2011 Concerning Funds Transfer is the law that governs money transfers in Indonesia (from now on, FT Act). The following parties are involved in the funds' transfer activities under this act:

1. Originator and Originating Provider

The person issuing the Funds Transfer Order in the initial instance is described as the Originator in Article 1 Number 7 of the FT Act. If applicable to the sale and purchase activity, an originator is a buyer who must make a financial transfer to the seller's account. An originator has a bank account (in FT Act termed as Originating Provider). A document in a default form provided by the bank to the customer binds the bank and the customer. Legal professionals refer to an agreement whose content has been standardized and put into a form as a standard-form agreement when created unilaterally. [Badruzaman, 1983](#)). Standard-form contracts are another name for standard-form agreements. A standard-form contract is

described as a "Preprinted contract with set clauses, frequently used by a business or within a certain industry with only minor changes or modifications to match the individual scenario" by Black's Law Dictionary. [Garner \(1999\)](#). According to Johannes Gunawan, a standard-form contract is one "in which the content, form and the close are developed, made, set, duplicated and distributed unilaterally, usually by business actors, without the approval of the other party, usually consumers" in [Gunawan \(2017\)](#).

2. The Beneficiary and the Beneficiary

A seller entitled to the money is referred to as the beneficiary. A beneficiary is the bank account owner (In FT Act, Article 1 Number 12 is termed Beneficiary Provider). The standard contract, a contract whose terms and conditions have been prepared and decided upon unilaterally by the user and bind the other party, forms the basis of the legal relationship between the owner of the bank account and the bank. The other side is unable to negotiate a change or alter it. In other words, the clauses that comprise the contract's terms and conditions are what are standardized here. [\(Sastrawidjaja, 2002\)](#)

3. Beneficiary and Sender

A sale and buy agreement establish the basis for the legal relationship between a sender and a beneficiary. According to Indonesian Civil Code Article 1457, a sale and purchase are an agreement wherein one party commits to delivering specific products in exchange for the other side paying the agreed-upon amount. According to Article 1457 of the Civil Code, a sale and buy agreement entails the following two obligations: [\(Harahap, 1986\)](#)

- a. The sender's obligation to deliver the purchased item to the customer
- b. The buyer's obligation to reimburse the seller for the agreed-upon amount

The sale and purchase agreement adopted in the civil code is required, so a sale and purchase agreement only outline the rights and obligations shared by the buyer and seller. The seller must transfer ownership of the goods he sells, giving him the right to demand payment of the agreed-upon price. On the other hand, it imposes a financial obligation on the buyer and grants him the right to request ownership of the item he purchases in exchange. "The ownership of the asset sold shall not be passed to the buyer until after delivery has a place, which shall occur in line with paragraphs 612, 613, and 616," according to Article 1459 of the Civil Code.

4. The Sending and Receiving Providers

The Funds Transfer Act is responsible for policing inter- and intra-provider transfers of funds within the Unitary State of the Republic of Indonesia and

international transfers of funds involving Indonesian service providers. Sending Provider and Receiving provider must be governed by the Money Transfer Act when conducting their funds' transfer activities. According to Article 1 Numbers 8 and 10 of the Funds Transfer Act, both are considered "funds transfer providers." The terms and conditions of Acceptance of the Funds Transfer Order that will be carried out later must be carefully read by the Sending Provider and Receiving Provider. When the sender and receiver's agreement, which forms the basis of the cash transfer, turns out to be fraudulent, issues arise. An agreement founded on fraud will not satisfy an agreement's condition, making the agreement worthless and voidable according to Article 1320 of the Civil Code, which outlines the requirements for the legality of agreements.

There should be a cancellation mechanism for the funds' transfer order and legal procedures to return the funds to the sender's account when the sender realizes that he has issued the funds' transfer order. Still, the recipient turns out to not be the one with the right to receive them because he has committed fraud. The laws governing financial transfers in Indonesia do not address this issue.

The Funds Transfer Act's flaws include the following:

i. Article 36, clause 1

If the Beneficiary Provider executes acceptance, it must be done immediately and on the same day that the previous Sending Provider received the Funds Transfer Order.

The sender may only cancel a Funds Transfer Order according to Article 42, paragraph (1) if the Beneficiary Provider has not taken the Acceptance actions specified in Article 36, paragraph, and the sender has received notice of the Beneficiary Provider's failure to take such action (2).

According to the abovementioned regulations, canceling a money transfer order requires giving the receiving provider enough time to complete the cancellation. However, the Beneficiary Provider is required to carry out acceptance right away. This demonstrates how challenging it is to cancel a transfer order.

Analysis of the Regulation of Opening a Bank Account in Indonesia

The fact that it is simple to register a bank account contributes to the difficulty of preventing online fraud cases. The government needs to pay attention to this. If a person complies with the bank's standards, they can open a bank account. When a customer has a bank account but is restricted by the bank, the consumer can still create an account with another bank, and the new bank is not aware of the customer's history of restrictions because of the alleged fraud. Many banks today even provide simple online

account opening options. Additionally, a client may have many accounts with the same bank.

According to Article 29 Paragraph, 2 of Act Number 10 of 1998 Concerning Amendment of Law Number 7 of 1992 Concerning Banking, which regulates the prudent banking principle, as well as Bank Indonesia Regulation Number 14/27/PBI/2012 Concerning Implementation of Anti Money Laundering and Combating the Financing of Terrorism Program for Commercial Bank, which has removed Bank Indonesia, a bank is bound to the prudent banking principle and the principle of knowing the customers. One effort to implement the prudent concept is the customer-knowledge principle. These bank rules, which include knowing the customer's identification and monitoring the customer's transaction activity, including reporting suspicious transactions, apply this principle:

- a. The customer acceptance policy;
- b. The customer identification policy and practices;
- b. The guidelines and practices for monitoring client accounts and transactions; and
- d. Risk management policies and practices connected to the idea of customer knowledge. [Rozali \(2011\)](#)

Since a bank first encounters a potential customer who plans to open an account, the Know the Customer Principle has been in place. In Articles 12 to 21 and Bank Indonesia Regulation Number 14/27/PBI/2012 concerning Implementation of Anti-Money Laundering and Combating the Financing of Terrorism Program for Commercial Bank, the notion of knowing the client applied by a bank is regulated. The procedures for accepting a customer (which begin with filling out a form containing information of the prospective customer's identity, income, source and use of the funds, signature specimen, etc.), identification and verification procedures (by analyzing the authenticity of documents and identifying the possibility of unnatural and suspicious things, cross-checking the information), and other measures are some that a bank should take to implement the principle of knowing the customer ([Erdiansyah, 2013](#)).

There are various scenarios where a bank customer opens an account and uses it to conceal money from fraud:

1. The offender creates an account using someone else's name.

According to Alfons Tanujaya, a security specialist at Vaksincom, the fundamental issue with the widespread creation of false accounts is how simple it is to obtain an identity card, including a real-looking but phony e-id. It is thought that information from the Civil Registry was compromised and sold online. When the voter registration information from the 2014

General Election leaked in May 2020; it was one of the most recent occurrences to make a big splash. There are 2.3 million citizens in total. The information is comparable to the Civil Registry information that can be used to create an e-ID, including the name, address, sex, and ID number. The offender can create a phony e-id using the information from the Civil Registry to open a bank account. The false e-photo id's is the perpetrator's photo to persuade the bank customer service [Hastuti \(2020\)](#).

Second, it's conceivable that the offender takes the victim's ID card. Many people's personal information leaks and is available for sale. You can utilize this. The account is then created and sold," said Heru Sutadi, a cyber security researcher at the Indonesia ICT Institute. The third method involves the offender hacking into the victims' digital platforms and stealing their identities. Finally, the culprit assists a bank employee so that opening a bank account is simple. ([Annur, 2020](#))

2. The account used is the legitimate one bearing the offender's identity. The offender is a client who legitimately holds a bank account. The bank can open the account per its Standard Operating Procedure and keep the prudential rule as prescribed by the law.

Act Number 23 of 1999 Concerning Bank Indonesia, Act Number 21 of 2011 Concerning Financial Services Authority, and Act Number 7 of 1992 Concerning Banking Jo are the laws that regulate banking. The limitation of customers' accounts, which allows one customer to have multiple accounts in the same bank as well as multiple accounts in other banks, is not regulated by Act Number 10 of 1998 concerning Amendment by Act Number 7 of 1992 concerning Banking, Act Number 21 of 2008 concerning Sharia Banking, Bank Indonesia Regulation, Regulation of Financial Services Authority, and Circular Letter of Bank Indonesia and Circular Letter of Financial Services Authority. (Written in cursive)

Analysis of the Procedure of Law Enforcement of Bank Account Misuse

In Indonesian banking practice, the victim must get in touch with the recipient provider by phone or email to resolve fraudulent financial transfer issues. The bank that receives the funds will conduct an early inquiry through customer care, request proof of the fraud, and then assist in blocking the offender's account. The following are the guidelines that serve as the foundation for account blocking activity:

According to Bank Indonesia Regulation Number 2/19/PBI/2000 concerning Requirements and Procedures to Grant Written Orders or Approval to Disclose Bank Secrets ("PBI 2/19/2000"), Article 12 paragraph (1), "Blocking and confiscating deposits owned by a person determined to be a suspect or a convict by the police, attorney, or judge, can be performed as set forth by the rules and regulations without the consent of the Governor of Bank Indonesia."

2. Section 26 of Act No. 8 of 2010, which prohibits and eradicates the crime of money laundering

a) The financial service provider may postpone transactions for a maximum of 5 (five) working days following the occurrence of the following:

a. completes the transaction;

b. keeps track of assets acquired through the criminal activity as described in Article 2 Section 1; or

c. is acknowledged and/or a valid allegation that they used a forged document.

According to the rules, the blocking process can only be carried out when the criminal law process has been completed. Additionally, the transaction postponement mechanism has no bearing on law enforcement efforts to stop fraud but is used to prevent money laundering.

Customers who contact the bank with a complaint must receive the following services:

1. Every bank must maintain a section mainly formed in every bank office to resolve customer complaints without being charged under Financial Services Authority Regulation No. 1/2013 concerning Protection for Consumers in the Financial Services Sector. The complaint must be founded on a monetary loss or potential loss for consumers brought on by the bank's error or negligence.

2. Following Bank Indonesia Regulation No. 7/7/PBI/2005 about the Settlement of Customer Complaint, the complaint may be made verbally or in writing at any bank office, regardless of whether the office is where the customer opens an account or completes a financial transaction.

3. Since the complaint is documented, the bank has two working days to resolve an oral complaint. If it is anticipated to take longer than expected, the bank's officer in charge of handling complaints may request in writing from the client.

4. The bank must respond to written complaints from customers within 20 (twenty) working days after receiving them, though this deadline may be extended under specific circumstances to 20 (twenty) working days.

5. The resolution of a customer's complaint may take the shape of an apology or financial compensation. When the following conditions are met: I the customer has fulfilled the obligation; (ii) there is a discrepancy between the product and/or bank service received and the terms of the

agreement; (iii) the complaint is filed within 30 days of discovering the discrepancy between the product and/or bank service and the agreement; and (iv) the loss directly affects the customer; compensation is given for a material loss. The Financial Services Authority determined the compensation at the same level as the customer's loss.

Since the bank only executes valid funds transfer orders, it cannot be held liable in cases of fraudulent funds transfers. According to Article 15 paragraph (1) of the Funds Transfer Act, the Original Sender Organizer may accept the Funds Transfer Order if they meet the following criteria:

- a. The Funds Transfer Order includes the information stated in Article 8 Paragraph 1 except for the Final Beneficiary Organizer's information for cash transfers of funds;
- a. The Original Sender has made available enough monies;
- c. The original sender organizer performed authentication; and
- d. The Funds Transfer Order complies with all applicable laws and regulations.

The bank has no obligation to bear liability for transfers made due to fraud. The bank must bear responsibility if the undertaker and crew make a mistake. The legal foundation is:

A. Consumer Protection Regulation Number 16/1/2014 of Bank Indonesia. "The Provider must be accountable for the consumer's damage caused by the faults made by its management and staff," the rule states in Article 10.

b. According to Article 29 of Financial Services Authority Regulation Number 1/PJOK.07/2013, "Financial Services Business must be responsible for the loss of the consumer caused by the errors and/or negligence of the management and employees of the Financial Services Business and/or third parties working on the Financial Services Business."

Since a funds transfer based on fraud is usually the mistake or carelessness of the sender, a bank will never promise to make a refund. Instead, the bank only serves to facilitate the early investigation by temporarily blocking the perpetrator's account and requesting that the police report be followed up further.

When fraud has already occurred and the funds' transfer process has been completed, the harmed party must proceed through a criminal law process, beginning with the step of filing a police report. The law enforcement process for a fraudulent act begins with a reporting procedure to the police, which the victim can do. The Investigator is permitted to obtain a report following Article 5, number 1 letter a, and Article 7, number 1 letter an of the Criminal Code. Investigator will carry out several investigations

following the report. When there are internet scams, the authorities will check for the Internet Protocol address as part of their investigation to identify the perpetrator. He will, after that, be taken into custody and subjected to a criminal code-compliant examination. The government must control different preventive procedures since there are still many barriers to the oppressive law enforcement of internet scams.

According to Lawrence M. Friedman, empowering the law entails strengthening the three facets of the legal system. The legal system comprises a structure, content, and cultural components. A legal system is a combination of "basic rules" (behavioral norms) and "secondary rules," according to L.A. Hart (norms about that norms-how to decide whether they are valid, how to enforce them, etc.). (Friedman, 1975). According to Lili Rasjidi and I. B. Wysa Putra, the law can be used to achieve protection that is not just adaptive but also anticipatory and predictive. (Rasjidi, 1993)

The Ministry of Communication and Informatics has received at least 192,000 (one hundred and ninety-two thousand) notifications about accounts accused of criminal activity since January 2020. At least 110,000 (one hundred and ten thousand) of these reports concern accounts charged with online fraud. Wikanto (2020) This demonstrates that Indonesian law enforcement, particularly the criminal statute against internet fraudsters, has not been carried out to its full potential. Therefore, the component of oppressive legal protection in defending the victims' rights would still need to be strengthened by offering simple and accessible processes and procedures for criminal reports.

Legal protection for victims is not just associated with oppressive measures or law enforcement efforts after the fact. Legal protection also includes preventative measures, which implies that it works to stop a conflict from occurring. (Hadjon, 1987) By visiting the cekrekening.id website supplied by the Ministry of Communication and Informatics, Indonesians can currently protect their losses due to online fraud. This website serves as a hub for the database of bank accounts that are thought to be used in illegal activity. This website exclusively gathers data so users can perform background checks before engaging in transactions or sending funds to specific bank accounts. The check outcome will indicate whether or not the account number has previously been implicated as belonging to a criminal. If it is simple for the perpetrator to use another account, use another person's account, and/or open a new account in a different bank, which allows the fraudulent act to continue, then using a website becomes ineffective.

In addition to the website run by the Ministry of Communication and Informatics, the government offers a system for managing public service complaints through the website lapor.go.id. This represents an effort to practice good governance. The website lapor represents the National Public Service Complaint System.go.id and is based on Presidential Regulation Number 76 of 2013 concerning Public Service Complaint

Management and Ministerial Regulation Number 3 of 2015 concerning the Roadmap of the National Public Service Complaint System Advancement. According to information spread online, the website lapor.go.id can be used to report online scams. In actuality, because the online is not controlled by law enforcement or the police, the "complaint" option on the web is not the way to begin the criminal law enforcement steps.

Based on the discussion in this part, the authors believe that the Indonesian legal system has to be backed by an organized, comprehensive policy to protect those who have been the victims of internet fraud. It is insufficient that the Electronic Information and Transactions Act has a criminal penalty. Indonesian legislation needs a straightforward law enforcement system to increase the victims' awareness of how to handle fraud situations they encounter.

Implications

Theoretical Implications

The theoretical ramifications of this study are significant because past research on bank fraud in online transactions has largely been ignored. This study significantly emphasizes in the literature how important it is to research bank policies to build the laws in a way that would give banks a framework of security and improve their performance. The contribution of this study to the body of knowledge would offer several alternative approaches that greatly appeal to the banking sector, and this study also aligns the literature with pertinent data. Future research would be advanced, and we would learn more about bank account abuse, thanks to the difficulties brought up throughout this study's discussion. To comprehend the addressed issues in online transactions and account security, the future study would benefit from focusing on the literature and the creation of successful techniques. This study would also add to the body of knowledge and expand the literature because it highlights the most recent and comprehensive information on online banking fraud.

Practical Implications

Due to the lack of a sizeable earlier study to combat financial fraud, the practical implications of this study are equally crucial. This study would improve the literature and theory in this area from practitioners' perspectives. This study aims to highlight the function of law enforcement and bank administration in securing public accounts and reducing the possibility of fraud in online transactions. The consequences of this study are significant in this sense because they detail several forms of online fraud. The banking industry can also strengthen the security of online transactions in light of this study to give customers more precise and realistic information. The results of this study can be generalized, and more accurate information can be generated to improve the security of the banking sector globally. Thus, its consequences are not just confined to

local banks. This study is critical because it contains thorough information about online transaction fraud and because its findings show that effective management and stakeholder activities can reduce online banking fraud.

Conclusions

It is possible to conclude that there are still legal policies that are not integrated based on the study of the core provisions of Indonesian laws and regulations, including banking laws, money transfer laws, and electronic information and transaction laws. This circumstance leads to inadequate legal protection for internet scam victims. Integrating policies must be the foundation for combating online fraud as a crime (penal and non-penal policies). The government has specified the punishments for the offenders. The penal policy has been put into practice by making the actions illegal in this situation. Conversely, a non-punitive strategy is equally necessary as a repressive and preventative tool. The government must establish account opening guidelines, banking sector standards, and a system for blacklisting the identities of account holders whose accounts have been used to commit fraud. Additionally, the government must offer more user-friendly and convenient ways for citizens to report crimes. To solve the issues, it is suggested that:

1. The government create a system of the criminal act online report using a trustworthy information technology system so that the information gathered can be identical to that recorded using the traditional report method.
 2. Establishing a fully integrated interbank customer data system that serves as a repository for data on consumers who have been identified as perpetrators of online fraud is necessary. This will make it difficult for consumers who have committed fraud to create a new account with a different bank.
1. To stop a fraudster from using many bank accounts to commit his crime, the number of accounts that one individual is allowed to have must be limited.

Future Directions

The misuse of bank transactions in Indonesia has been covered in this paper. This study has significantly contributed by highlighting many aspects of online transaction fraud. Therefore, future research must concentrate on how cybercrime policy helps prevent online banking fraud. Second, future research must clarify how strong bank security helps prevent online banking fraud. Last but not least, future research must concentrate on the connection between online and mobile banking fraud.

Reference

- Annur, C. M. (2020). IT Experts Reveal Four Modes of Buying and Selling Bank Account Books in E-Commerce. Retrieved from <https://katadata.co.id/desysetyowati/digital/5eff1abe07962>
- Arief, B. N. (1992). Anthology of Criminal Law Policy, Bandung: Alumni, 1992. Bandung: Alumni.
- Badruzaman, M. D. (1983). Bank Credit Agreement. Bandung: Alumni.
- Center., I. I. S. P. A. a. I. S. (2020). Report of Internet Survey APJII 2019-2020 (Q2). Retrieved December 21, 2020,. Retrieved from <https://apjii.or.id/survei>,
- Christiani, T. A. (2016). Normative and Empirical Research Methods: Their Usefulness and Relevance in the Study of Law as an Object. *Procedia - Social and Behavioral Sciences*, 219, 201-207. doi:<https://doi.org/10.1016/j.sbspro.2016.05.006>
- Contributors., C. (2021). Kominfo Records Most Online Fraud Cases: Selling Online. Jakarta: CNN Indonesia. Retrieved from <https://www.cnnindonesia.com/teknologi/20211015085350-185-708099/kominfo-catat-kasus-penipuan-online-terbanyak-jualan->
- Demirgüç-Kunt, A., Pedraza, A., & Ruiz-Ortega, C. (2021). Banking sector performance during the COVID-19 crisis. *Journal of Banking & Finance*, 133, 106305. doi:<https://doi.org/10.1016/j.jbankfin.2021.106305>
- Erdiansyah. (2013). Application of Know Your Customer Principles as a Form of Bank's Role in Anticipating Money Laundering at PT. Bank Negara Indonesia (Persero) Tbk Pekanbaru Branch. *Riau Legal Science Journal*, 3(1), 7-13. Retrieved from <https://www.neliti.com/publications/9141/penerapan-prinsip-mengenal-nasabah-sebagai-bentuk-peranan-bank-dalam-mengantisipasi#cite>
- Friedman, L. M. (1975). *The legal system: A social science perspective*: Russell Sage Foundation.
- Garner, B. A. (1999). *Black's Law Dictionary*, Seventh Edition. Eagan, Minnesota: West Group Publishing.
- Gunawan, J. (2017). Reorientation of Contract Law in Indonesia., *Journal of Business Law*, 22(6), 45.
- Hadjon, P. M. (1987). Legal Protection for the Indonesian People. Surabaya: Science Development. In: Hlm.
- Harahap, M. Y. (1986). Aspects of Contract Law. Bandung: Alumni.
- Hastuti, R. K., & Astutik, Y. (2020). Chaotic! Asphalt e-KTP Behind Making Illegal Bank Accounts. Jakarta: CNBC Indonesia. Retrieved December 28, 2020. Retrieved from <https://www.cnbcindonesia.com/tech/20200706141553-37-170526/kacau-e-ktp-aspal-di-balik-pembuatan-rekening-bank-illegal>
- Hidajat, T., & Lutfiah, N. (2022). E-Wallet: Make Users More Consumptive? *ECONBANK: Journal of Economics and Banking*, 4(1), 15-22. doi:<https://doi.org/10.35829/econbank.v4i1.163>

- Ismanto, H., Widiastuti, A., Muharam, H., Pangestuti, I. R. D., & Rofiq, F. (2019). *Banking and financial literacy*: Deepublish.
- khan, M. M. S., & Ghayas, M. M. (2022). Impact of authentic leadership on employee engagement in the banking sector of Karachi. *International Journal of Business Performance Management*, 23(1-2), 90-98. doi:<https://doi.org/10.1504/ijbpm.2022.119567>
- Lee, M.-C. (2009). Factors influencing the adoption of internet banking: An integration of TAM and TPB with perceived risk and perceived benefit. *Electronic Commerce Research and Applications*, 8(3), 130-141. doi:<https://doi.org/10.1016/j.elerap.2008.11.006>
- Lutfiyana, A. (2021). Online Buying and Selling Fraud in Indonesia and Its Criminal Law Enforcement. *Law Research Review Quarterly*, 7(1), 53-68. doi:<https://doi.org/10.15294/lrrq.v7i1.43192>
- Marzuki, P. M. (2005). Legal Research. Jakarta: Prenada Media.
- Rahmanto, T. Y., Kav, J., & Kuningan, J. (2019). Law Enforcement Against Fraud Based on Electronic Transactions. *De Jure Legal Research Journal*, 19(1), 31. doi:<http://dx.doi.org/10.30641/dejure.2019.V19.31-52>
- Ramadhani, P. I. (2020). Bareskrim Records 1,617 Online Fraud Cases in 2019 the Most on Instagram. *Liputan6. com*, 29. Retrieved from <https://www.liputan6.com/bisnis/read/4369038/bareskrim-catat-ada-1617-kasus-penipuan-online-pada-2019-paling-banyak-di-instagram>
- Rasjidi, L., & Putra, I. W. (1993). Law as a System. Bandung: Rosdakarya Youth.
- Ravena, D., & Kristian. (2017). Criminal Policy,. Jakarta:: Kencana.
- Rozali, A. (2011). Know Your Customer Principles in Banking Practice. *Journal of Juridical Insights*, 24(1), 304. doi:<http://dx.doi.org/10.25072/jwy.v24i1.18>
- Sastrawidjaja, M. S. (2002). The Standard Covenant in Cyber Activities, Cyberlaw: An Introduction. *Jakarta: Ellipse II*.
- Setyaningsih, E. D., & Marwansyah, S. (2019). The effect of halal certification and halal awareness through interest in decisions on buying halal food products. *Syiar Iqtishadi: Journal of Islamic Economics, Finance and Banking*, 3(1), 65-79. doi:<http://dx.doi.org/10.35448/jiec.v3i1.5515>
- Shafique, O., & Khan, M. (2020). Factors Affecting Bankers' Behavioral Intention to Adopt Green Banking: An Empirical Analysis of Banks in Pakistan. *Journal of Business and Social Review in Emerging Economies*, 6(2), 835-843.
- Shaikh, S. A. (2018). Role of Islamic banking in financial inclusiveness in Pakistan: promise, performance and prospects. *International Journal of Financial Services Management*, 9(1), 88-102. Retrieved from <https://www.researchgate.net/profile/Salman-Shaikh-3/publication/323107855>
- Sufriadi, Y. (2021, 22-23 Sept. 2021). *Prevention Efforts Against E-Commerce Fraud Based on Indonesian Cyber Law*. Paper presented at the 2021 9th International Conference on Cyber and IT Service Management (CITSM).

- Wikanto, A. (2020). This is How to Check Fraudulent Accounts to Prevent Money Transfer Mode Crimes. *Jakarta: nasional.kontan.co.id. Retrieved.* Retrieved from <https://nasional.kontan.co.id/news/inicara-cek-rekening-penipuan-untuk-cegah-kejahatan-modus-transfer-uang>
- Younas, W., & Kalimuthu, K. R. (2021). Telecom microfinance banking versus commercial banking: a battle in the financial services sector. *Journal of Financial Services Marketing*, 26(2), 67-80. doi:<https://doi.org/10.1057/s41264-020-00085-7>